CLOUD NATIVE
COMPUTING FOUNDATION

Kyverno

Kubernetes Native Policy Management

March, 2023
Bangalore, India

nirmata

Agenda

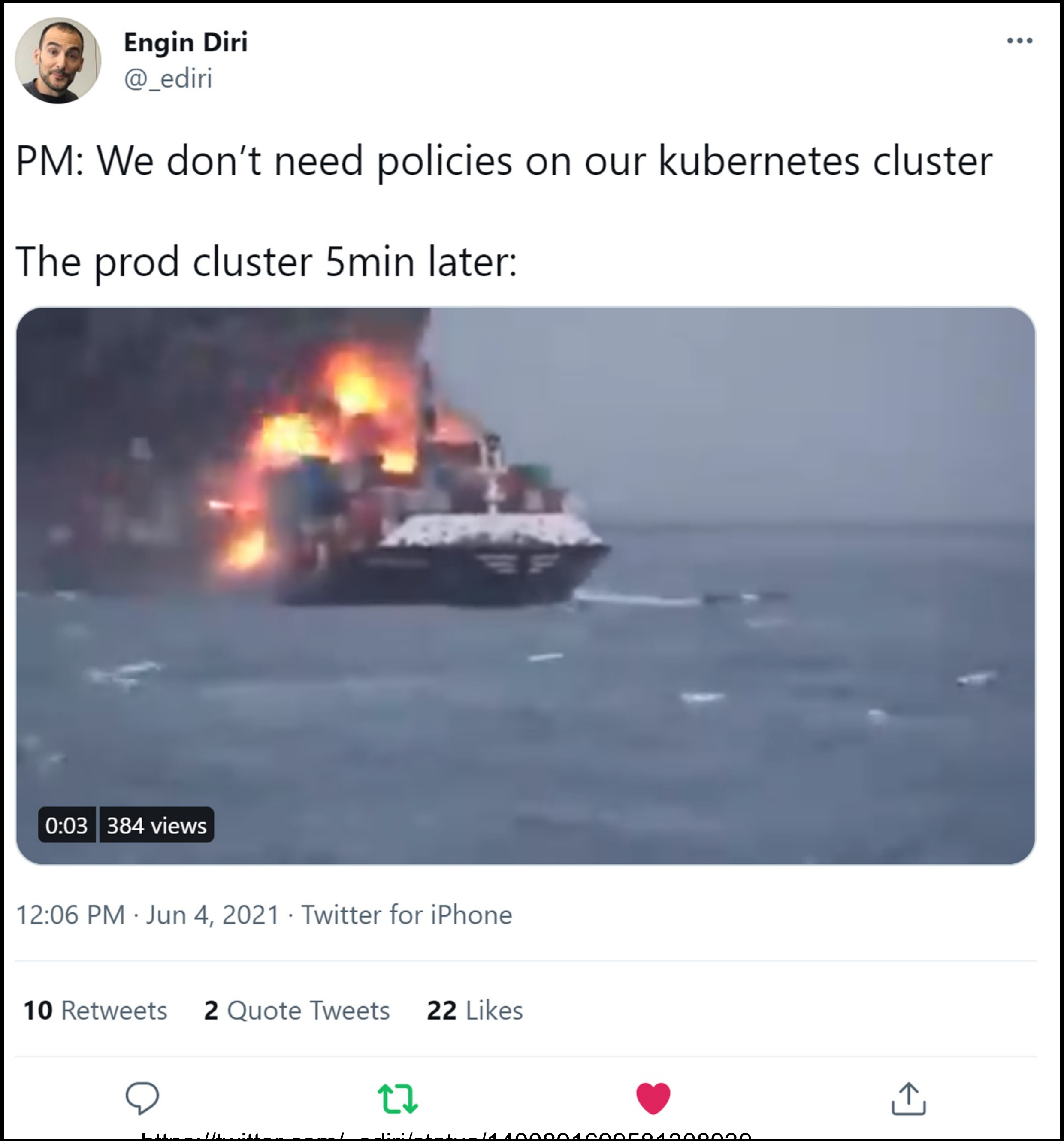
- Why Policies?
- Why Kyverno?
- How Kyverno polices work
- Demo
- Additional Features
- Summary
- Q&A

About me

- Co-founder and CEO, Nirmata
- Kyverno Co-creator and Maintainer
- Co-chair Kubernetes Policy and Multi-tenancy Working Groups

@JimBugwadia

Why policies?



Engin Diri
@_ediri

PM: We don’t need policies on our kubernetes cluster

The prod cluster 5min later:

12:06 PM · Jun 4, 2021 · Twitter for iPhone

10 Retweets **2** Quote Tweets **22** Likes

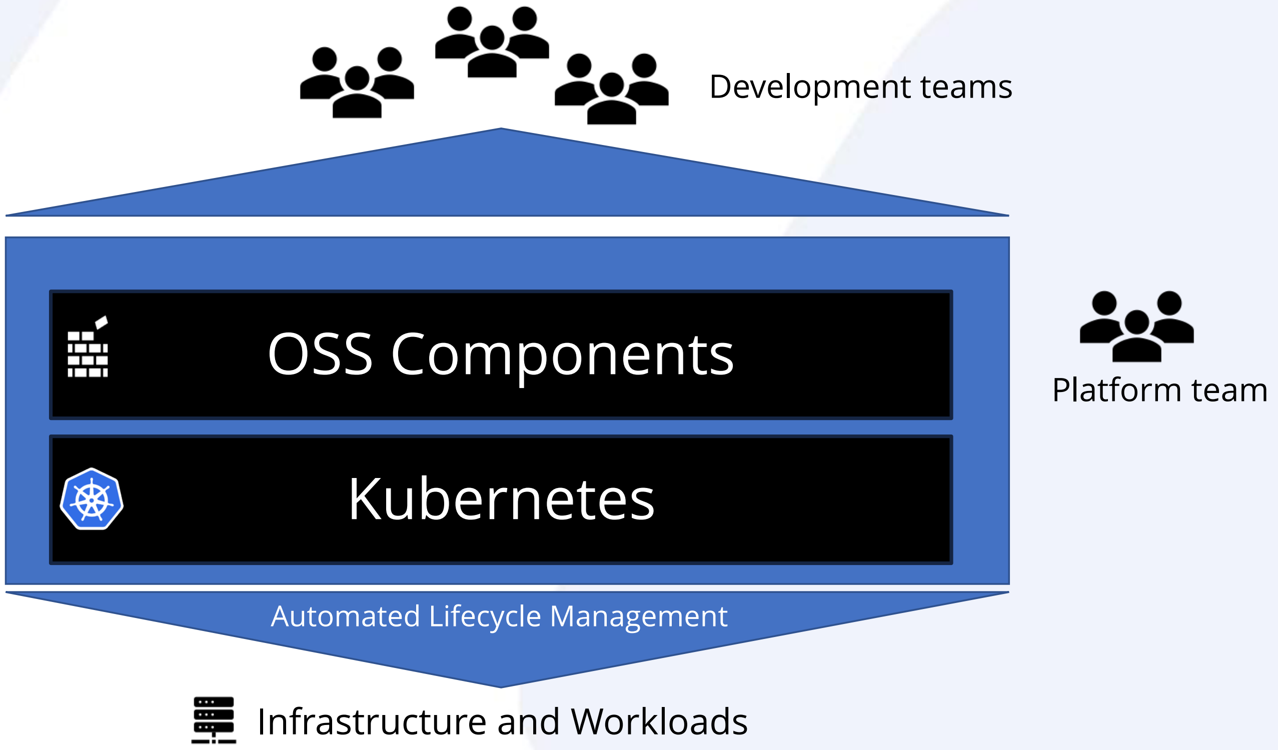
https://twitter.com/_ediri/status/1400891699581308929

The rise of Kubernetes platforms

By 2026, 80% of software engineering organizations will establish platform teams as internal providers of reusable services, components and tools for application delivery.

Source: Gartner

96% of enterprises are using or evaluating Kubernetes – CNCF survey



Development teams

OSS Components

Kubernetes

Platform team

Automated Lifecycle Management

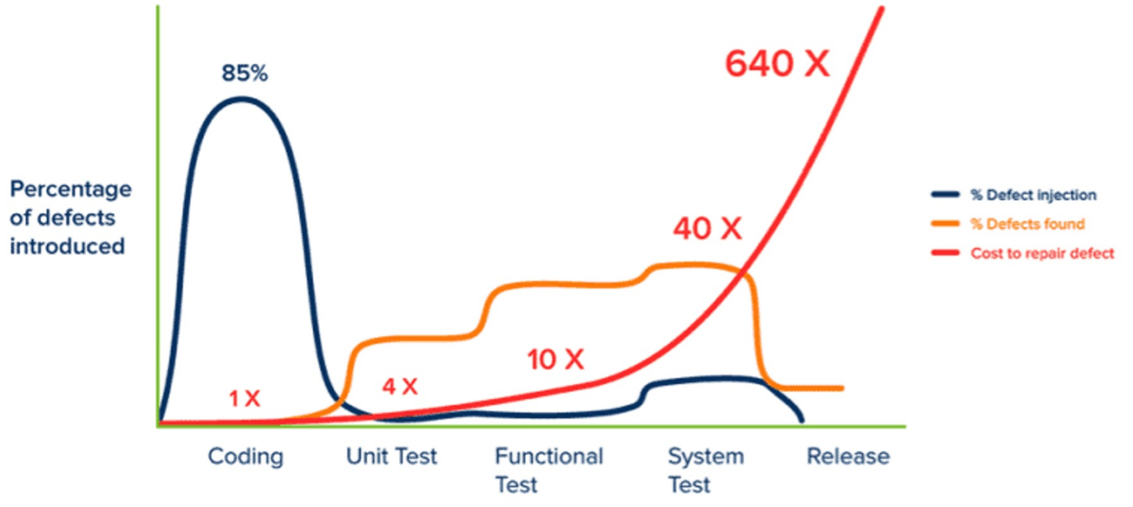
Infrastructure and Workloads

The cost of missing Kubernetes guardrails

328 average # of misconfigurations per cluster

110 average # of workloads per cluster

3 average # of findings per workload



Jones, Capers. *Applied Software Measurement: Global Analysis of Productivity and Quality.*

Phase	Pre-deploy	Production
Cost per defect	$25	$15,903
Cost per cluster	$8151	$5,216,193

https://www.cncf.io/blog/2022/02/02/the-cost-of-a-kubernetes-repair-in-development-vs-production/

Policies are a contract

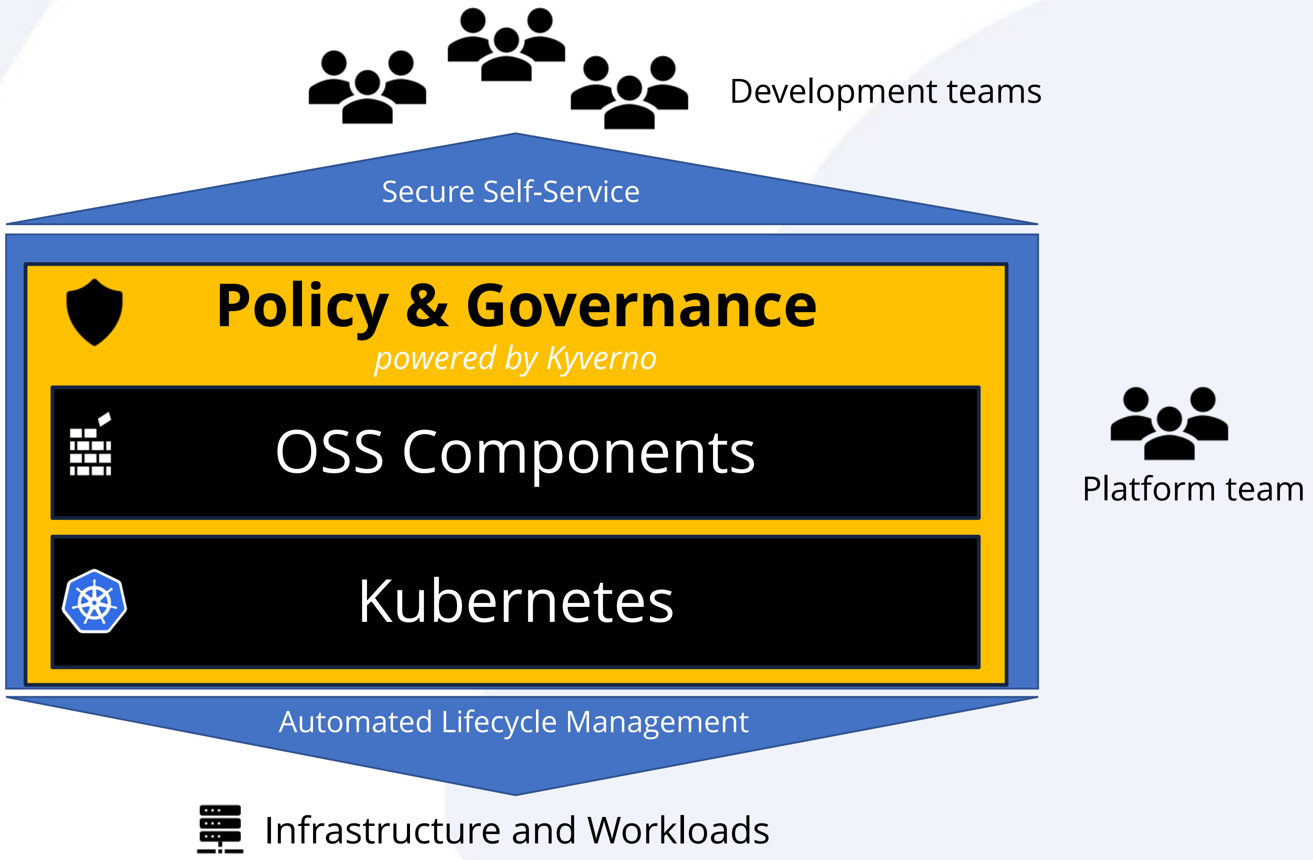
Developers ☑

Security ☑

Operations ☑

Kyverno enables Kubernetes platform teams

1. Policy-based guardrails for security and compliance
2. Automation of security and operational workflows
3. Flexible reporting and policy exception management


Development teams

Secure Self-Service

Policy & Governance

powered by Kyverno

OSS Components

Kubernetes

Automated Lifecycle Management

Platform team

Infrastructure and Workloads

What policies provide

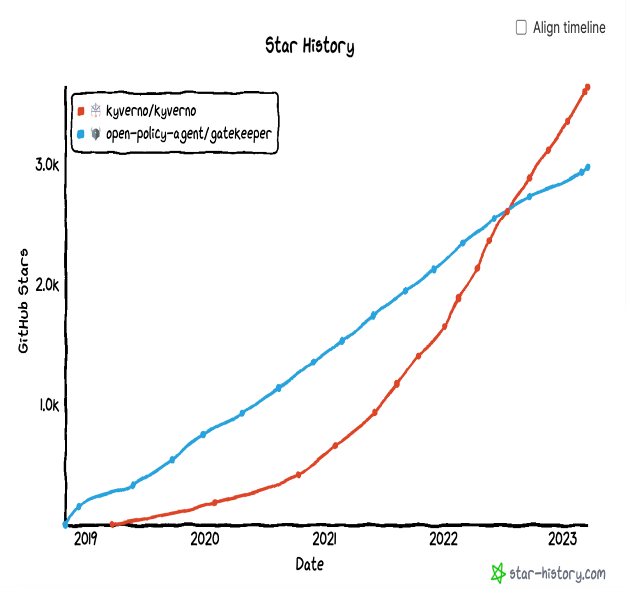
1. Separation of concerns across Dev-Sec-Ops roles
2. Security via validation and enforcement checks
3. Just-in-time automation

Why Kyverno?

Kyverno is the Kubernetes native policy engine

CNCF project created and maintained by Nirmata

- ☑ **Eliminate misconfigurations**
- ☑ **Prevent vs. detect**
- ☑ **Shift-left security**



- 1.3 Billion+ image pulls
- 3.6K+ GitHub Stars
- 300+ contributors
- 1700+ Slack members
- 230+ policies

Secureworks
NCR
Chick-fil-A
wayfair
GROFERS
Goldman Sachs
Discovery CHANNEL
Nextdoor
REPLY DATA
WILLIAMS SONOMA
talend
st1
CHAN ZUCKERBERG INITIATIVE
coinbase
GE Healthcare
zipcar
APEX Clearing DIGITAL WEALTH SOLUTIONS
ACTIAN
celonis
FXC intelligence
fastly
CERT MANAGER
Giant Swarm
VSHN
Bloomberg
OpenEBS
Litmus
OVHcloud
TQL TOTAL QUALITY LOGISTICS
flux
CNF Test Suite
MANDIANT
Deutsche Telekom Group
T · ·
sky Q
Vonage
vodafone
orange
zain

Why Kyverno?

Kyverno simplifies K8s policy management!

1. Make K8s policies easy to write and manage
2. Make policy results easy to process
3. Validate (audit or enforce), Mutate, and Generate
4. Support all Kubernetes types including Custom Resources
5. Use Kubernetes patterns and practices
   e.g. labels and selectors, annotations, events, ownerReferences, pod controllers, etc.

CNCF Policy Engines: Kyverno or OPA?

"Thank you all for Kyverno, It made K8s policy really easy, I struggled for months with OPA/Gatekeeper, I am glad I found Kyverno." – ***GKE admin on community forums***

Kyverno	OPA / Gatekeeper
Kubernetes-native	General purpose rules engine
Policies are declarative Kubernetes resources	Custom DSL (Rego) built for authorization
Validation	Validation
Mutation	--
Generation	--
Image Verification	--
Native CNCF standardized reporting	--
Use GitOps and other Kubernetes tools	--
Higher performance with lower resources	--

Kubernetes Policy Management Tools Compared OPA with Gatekeeper vs. Kyverno -- by Viktor Farcic

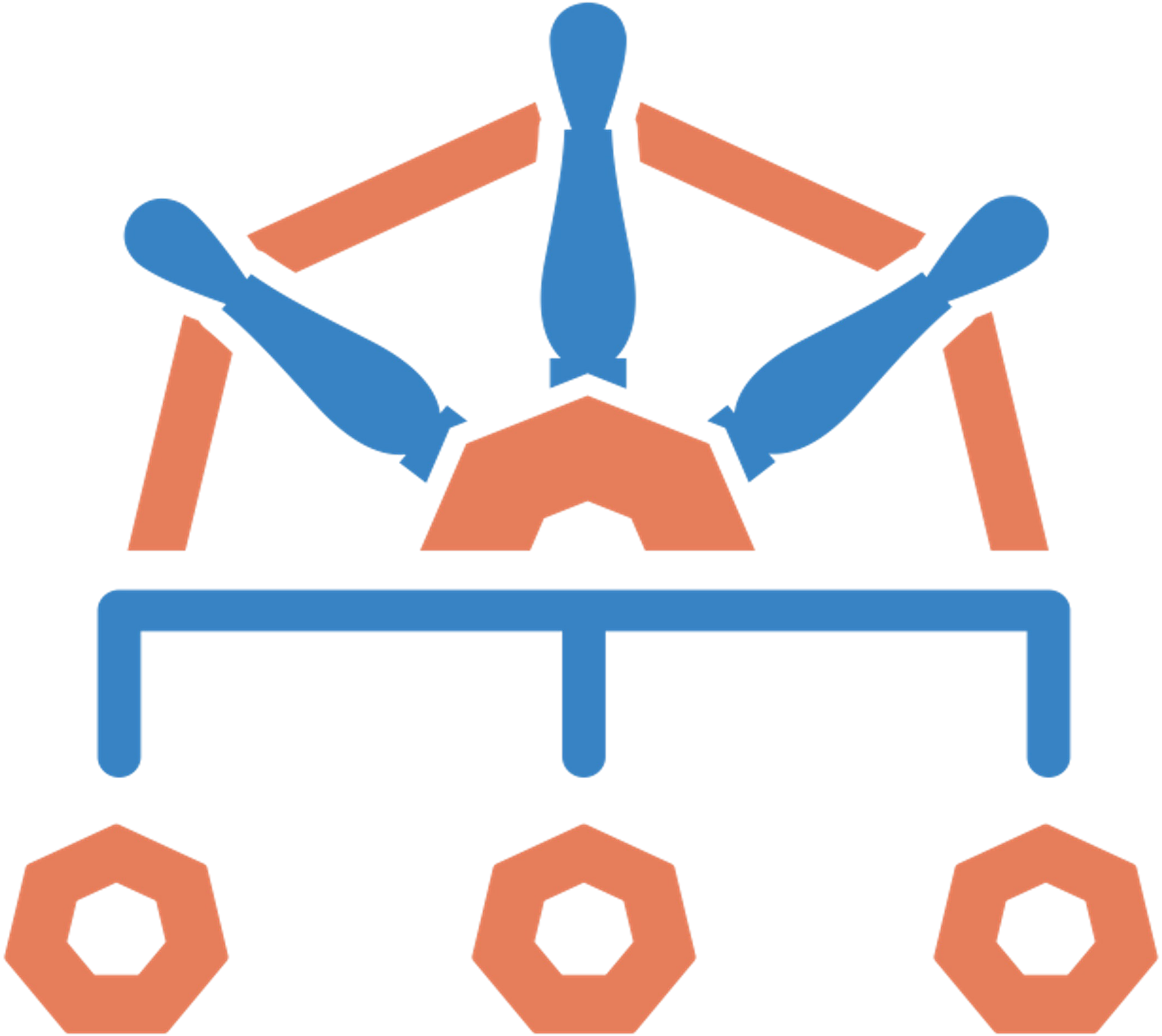
#Gatekeeper #OPA #Kyverno

Kubernetes Policy Management Tools Compared - OPA with Gatekeeper vs. Kyverno

1,390 views • Jul 1, 2021

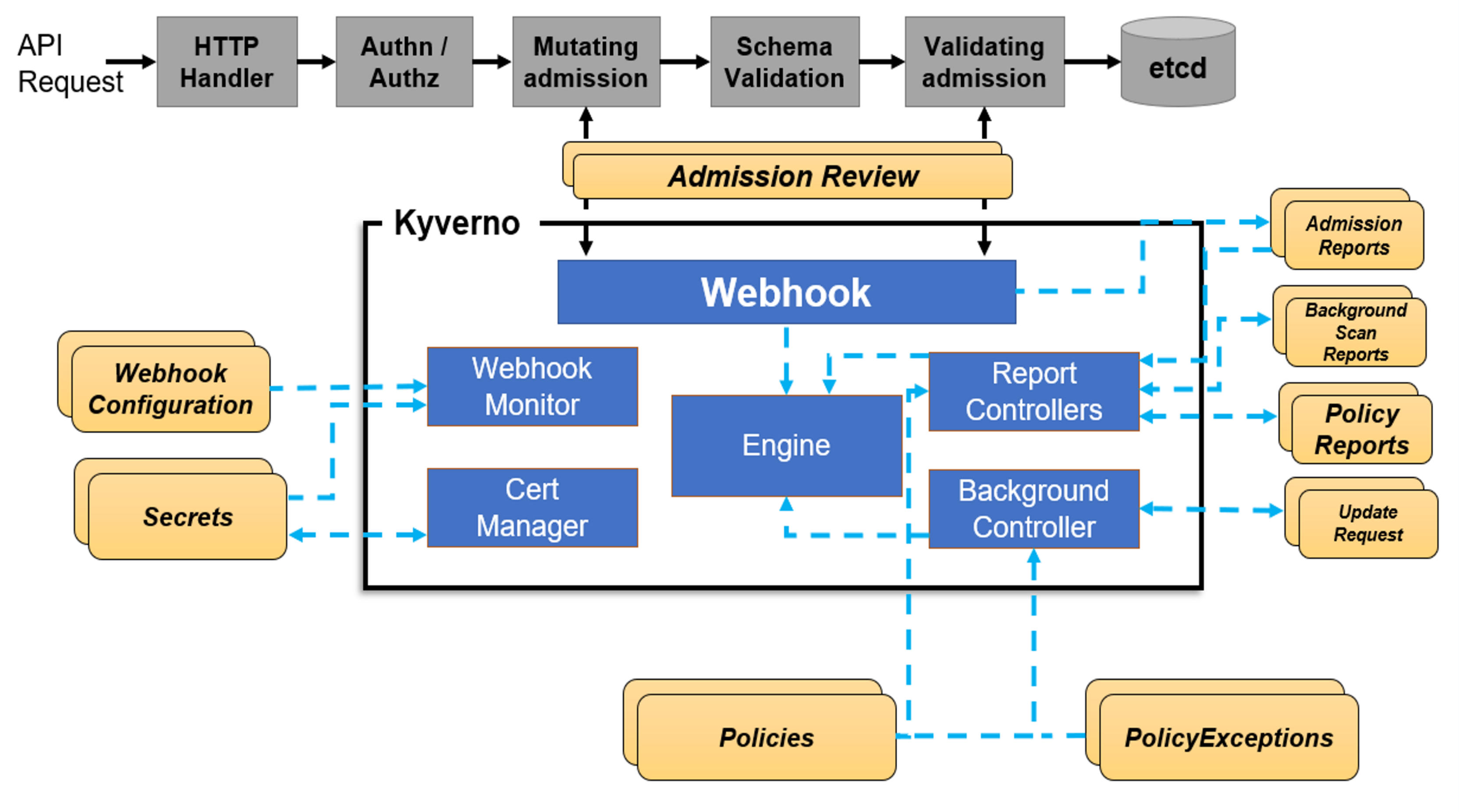
nirmata

How Kyverno Policies Work

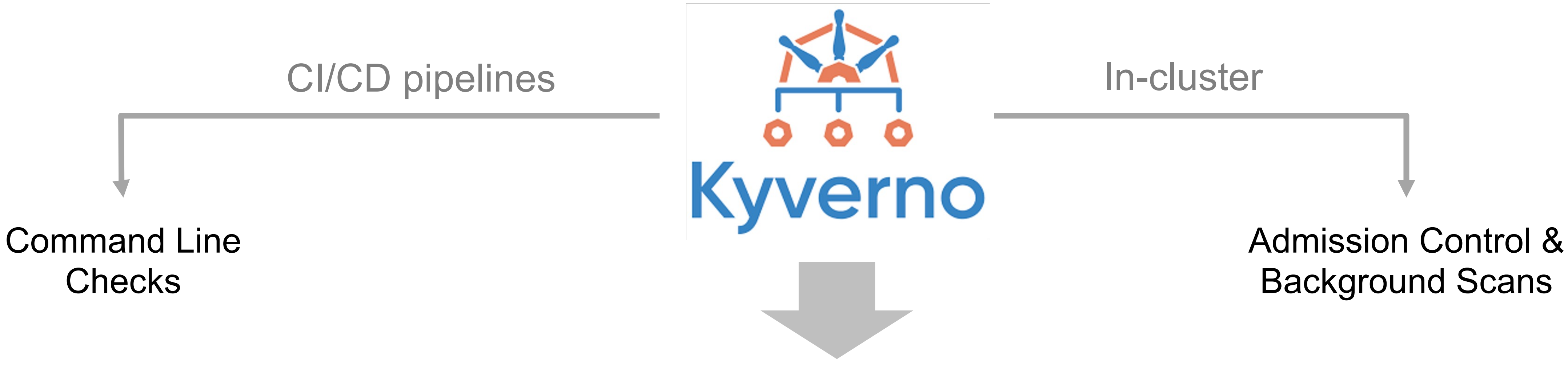


Kyverno Architecture

- ☑ Admission Controls
- ☑ Command Line (CLI)
- ☑ Runtime scans



Kyverno Policy Management Use Cases



CI/CD pipelines

Kyverno

In-cluster

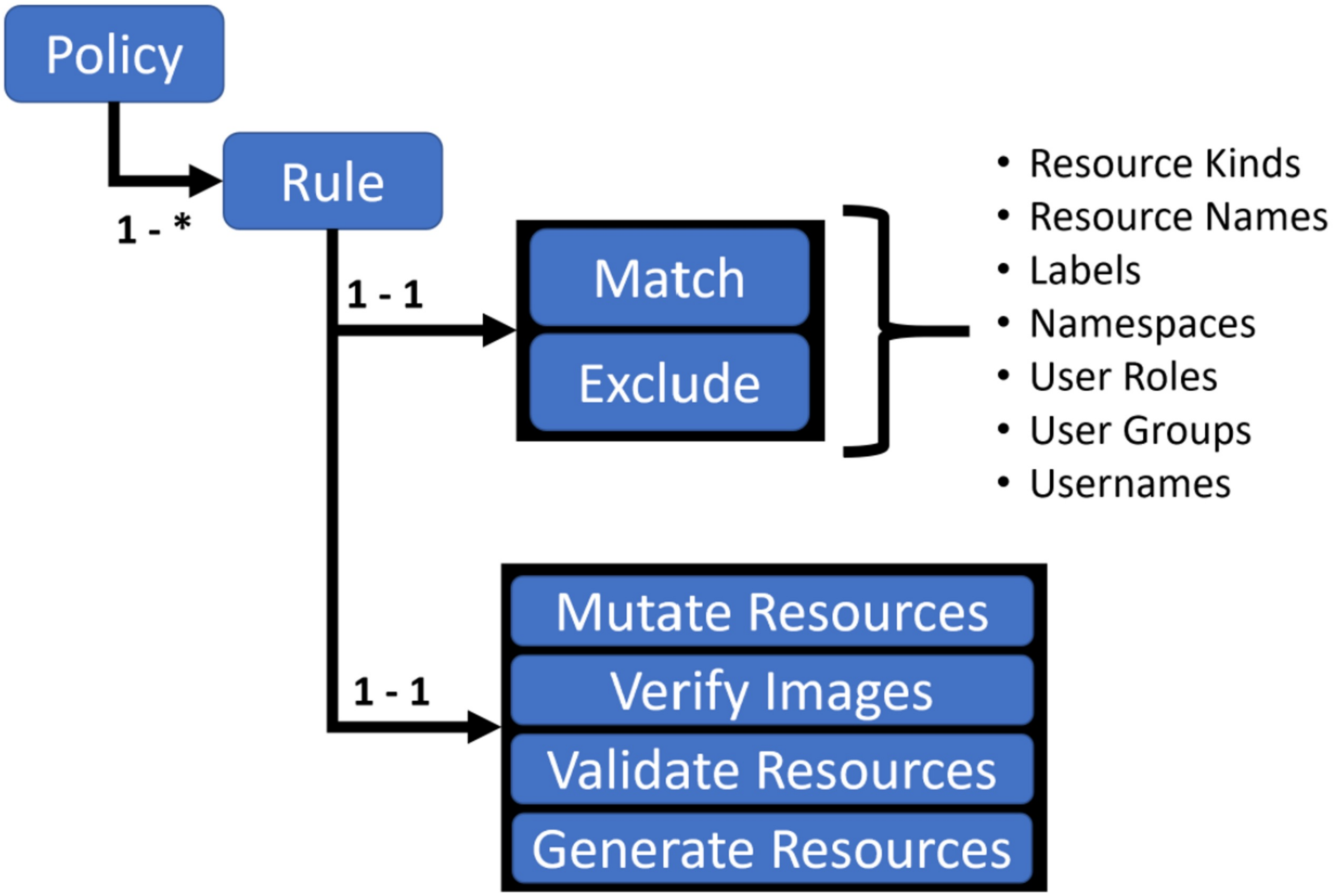
Command Line Checks

Admission Control & Background Scans

Top Use Cases

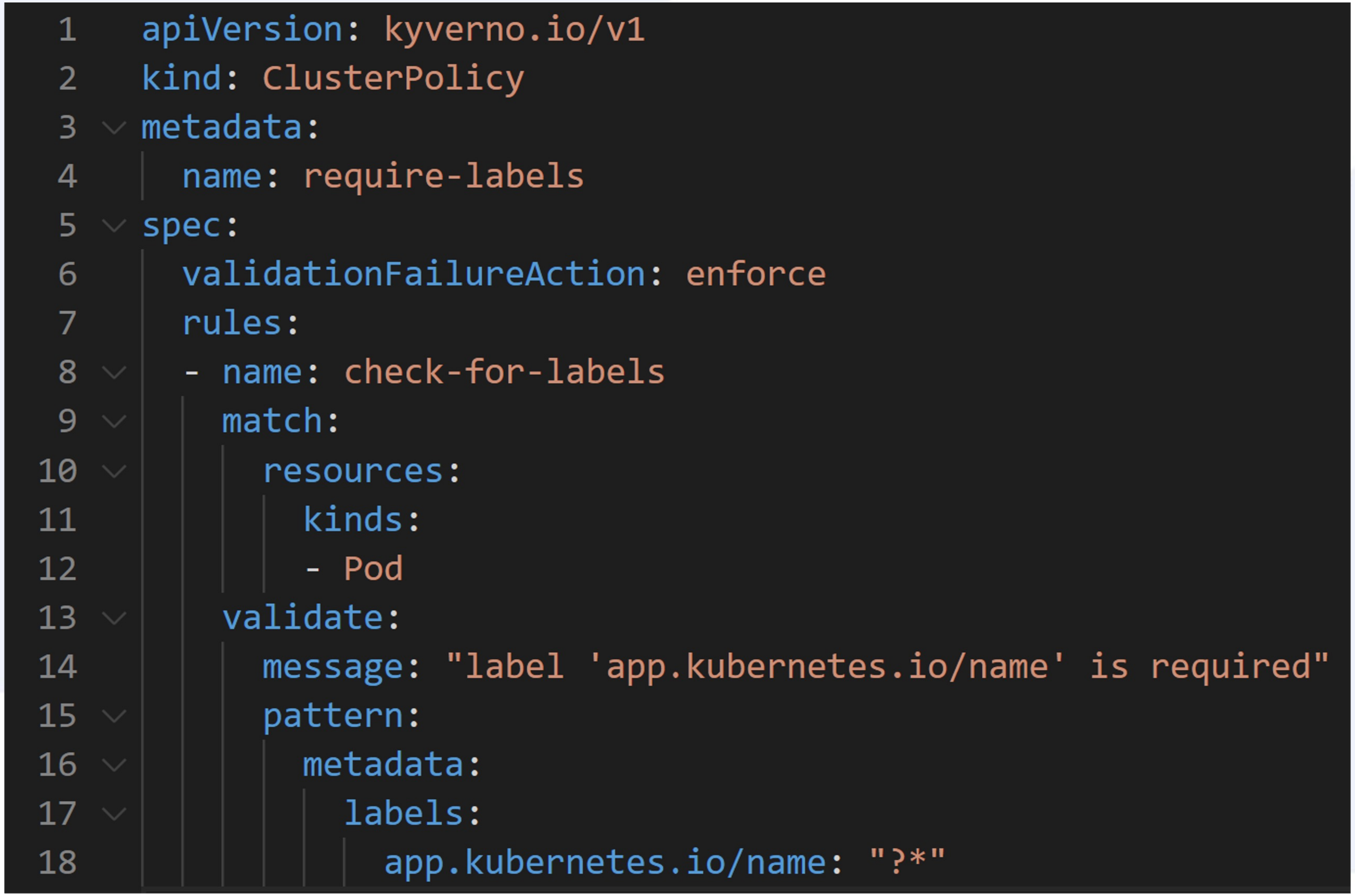
SecOps	DevOps	FinOps
• Pod security • Workload security • Granular RBAC • Workload isolation • Image signing & verification • Workload identity	• Self-service Kubernetes environments • Self-service infrastructure (IaC) • Resource governance and cleanup • Label/Annotation management • Naming conventions • Event driven automation • Custom CA management • Time-bound policies	• Quota Management • Pod Requests and limits • Team and app labels • Scaling limits • Scheduled resources • QoS management • Auto-scalers

A Kyverno Policy



- Resource Kinds
- Resource Names
- Labels
- Namespaces
- User Roles
- User Groups
- Usernames

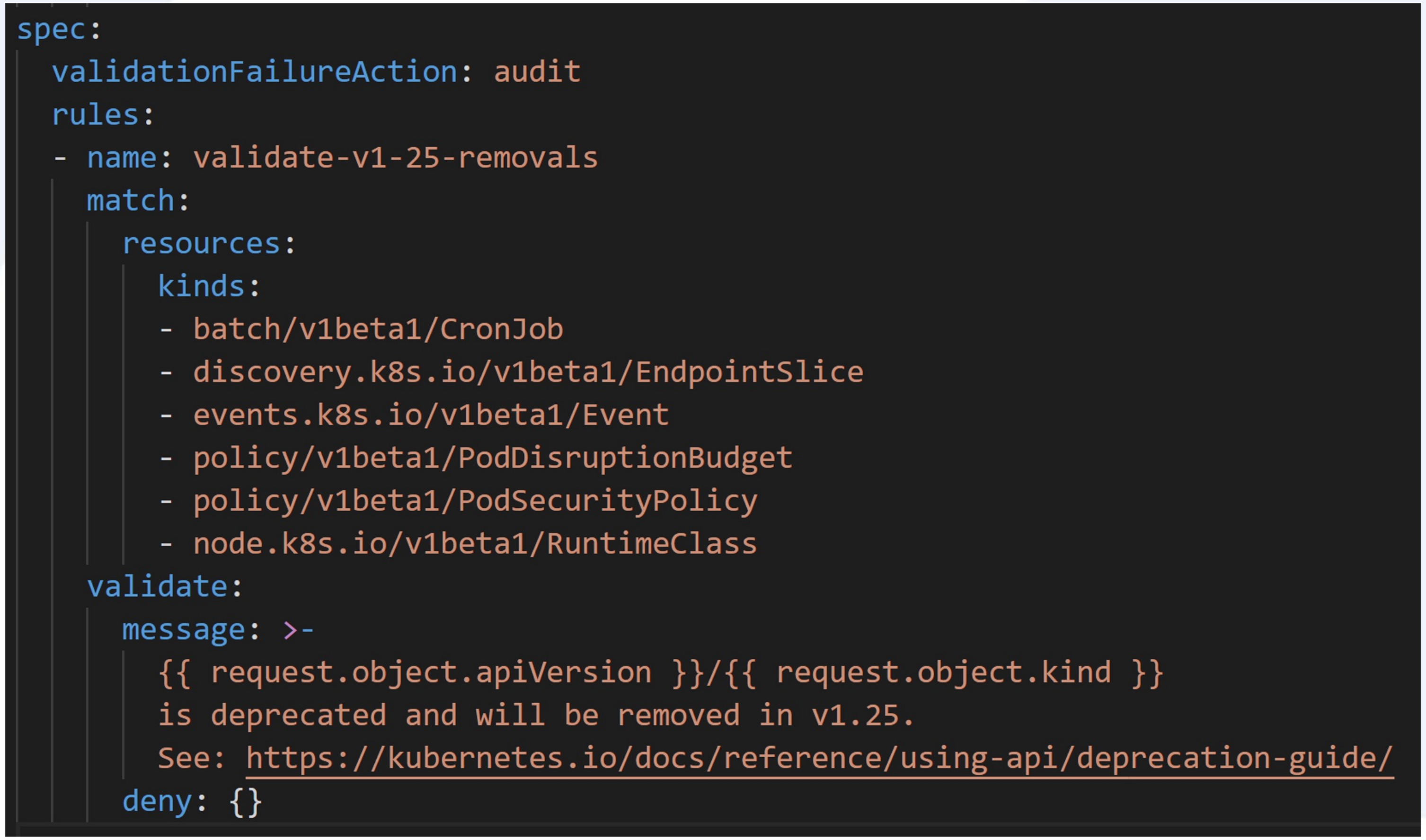
A Kyverno Policy



```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: require-labels
spec:
  validationFailureAction: enforce
  rules:
  - name: check-for-labels
    match:
      resources:
        kinds:
        - Pod
    validate:
      message: "label 'app.kubernetes.io/name' is required"
      pattern:
        metadata:
          labels:
            app.kubernetes.io/name: "?*"
```

Validate Policy

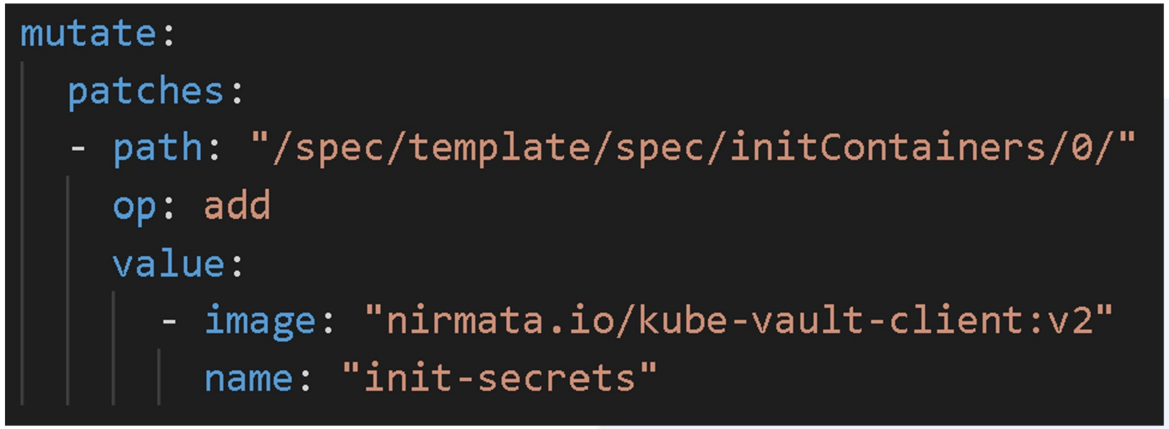
- Overlays with patterns specify desired state
- Matches all defined fields
- Patterns
    - * : zero or more
    - ? : any one
- Operators
    - >, <, >=, <=, !, | (or)



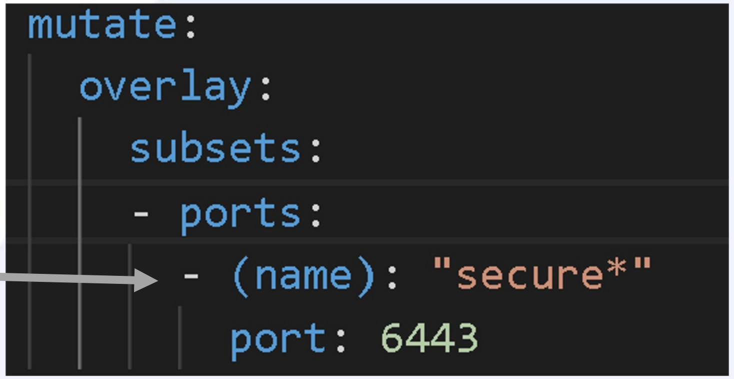
```yaml
spec:
  validationFailureAction: audit
  rules:
  - name: validate-v1-25-removals
    match:
      resources:
        kinds:
        - batch/v1beta1/CronJob
        - discovery.k8s.io/v1beta1/EndpointSlice
        - events.k8s.io/v1beta1/Event
        - policy/v1beta1/PodDisruptionBudget
        - policy/v1beta1/PodSecurityPolicy
        - node.k8s.io/v1beta1/RuntimeClass
    validate:
      message: >-
        {{ request.object.apiVersion }}/{{ request.object.kind }}
        is deprecated and will be removed in v1.25.
        See: https://kubernetes.io/docs/reference/using-api/deprecation-guide/
      deny: {}
```

Mutate Policy

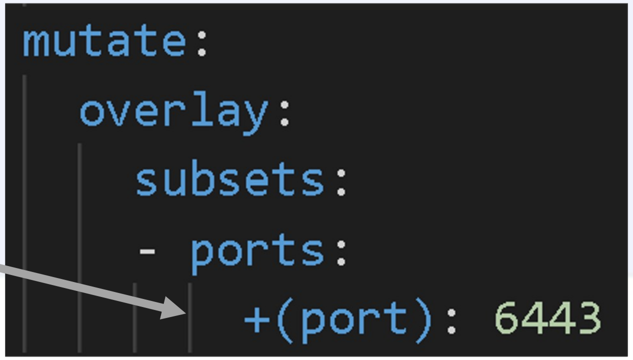
- JSON Patch (RFC 6902)
  - Use for precise updates
- StrategicMergePatch
  - Use for describing intent
  - Anchors for conditional logic
    - “If-then-else”
    - “if-not-defined”



```
mutate:
  patches:
  - path: "/spec/template/spec/initContainers/0/"
    op: add
    value:
      - image: "nirmata.io/kube-vault-client:v2"
        name: "init-secrets"
```



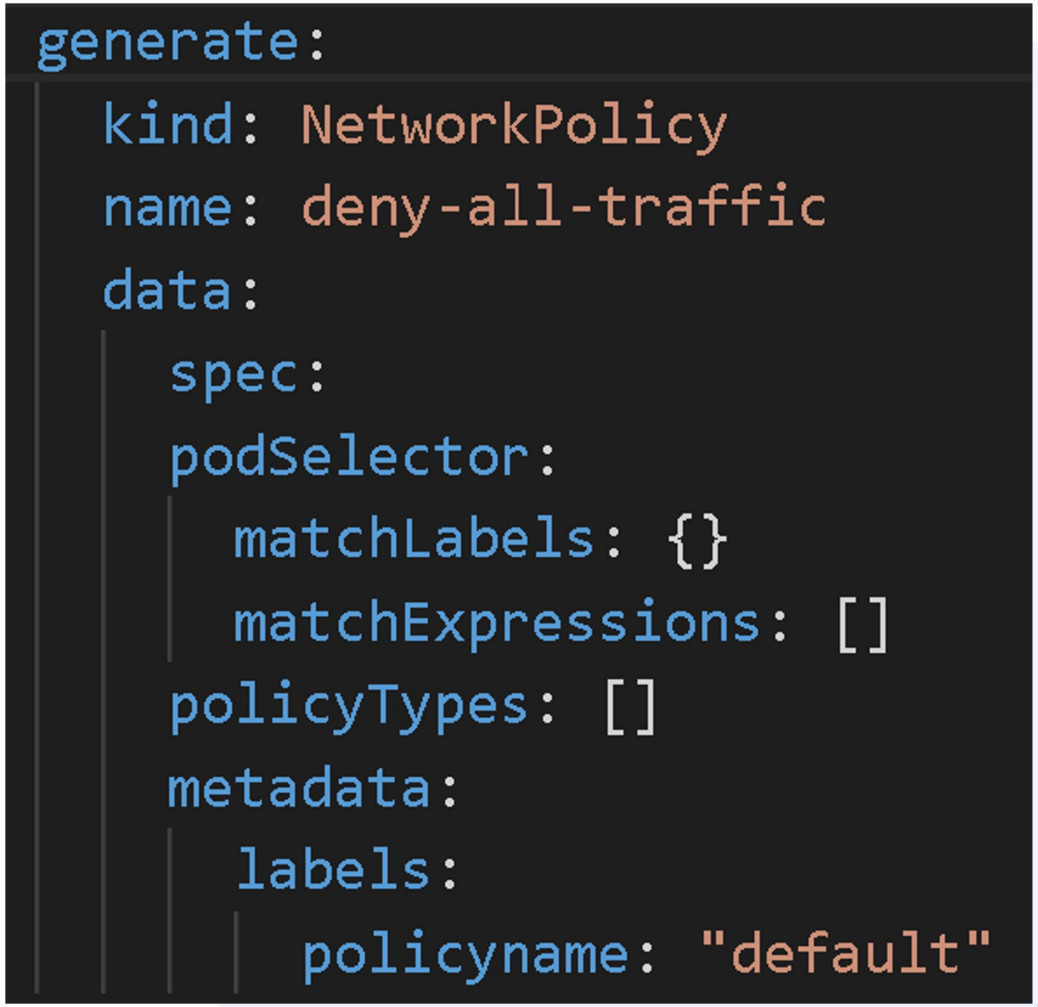
```
mutate:
  overlay:
    subsets:
    - ports:
      - (name): "secure*"
        port: 6443
```



```
mutate:
  overlay:
    subsets:
    - ports:
        +(port): 6443
```

Generate Policy

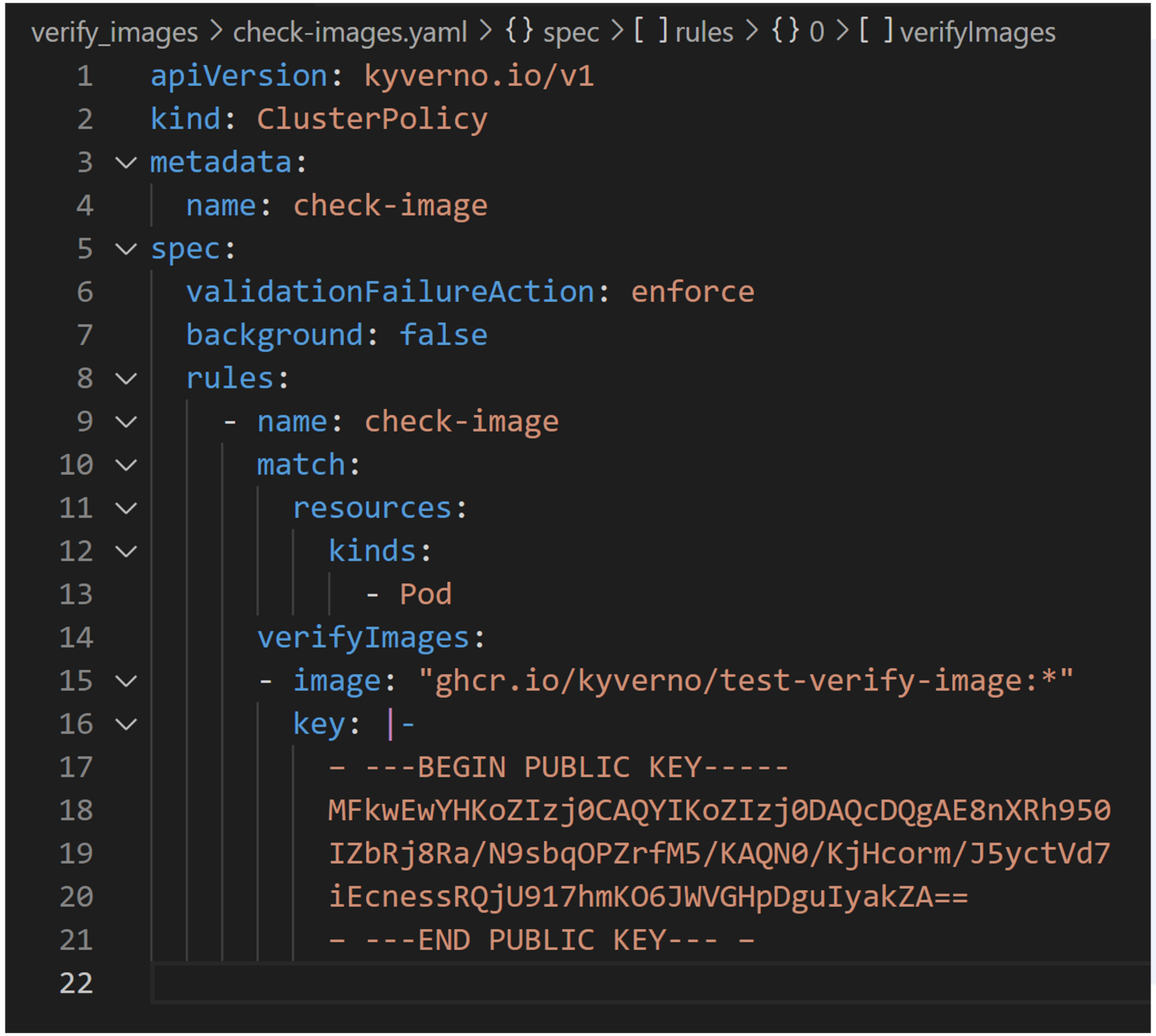
- Triggers when a new resource is created or based on label and metadata changes
- Useful in creating defaults for a namespace
- Clones existing resources or copies in-line data
- Can optionally keep data in-sync across namespaces



```
generate:
  kind: NetworkPolicy
  name: deny-all-traffic
  data:
    spec:
    podSelector:
      matchLabels: {}
      matchExpressions: []
    policyTypes: []
    metadata:
      labels:
        policyname: "default"
```

Image Verification Policy

- Native Sigstore support!
- Match images using wildcards
- Verify multiple signatures
- Optional signature registry



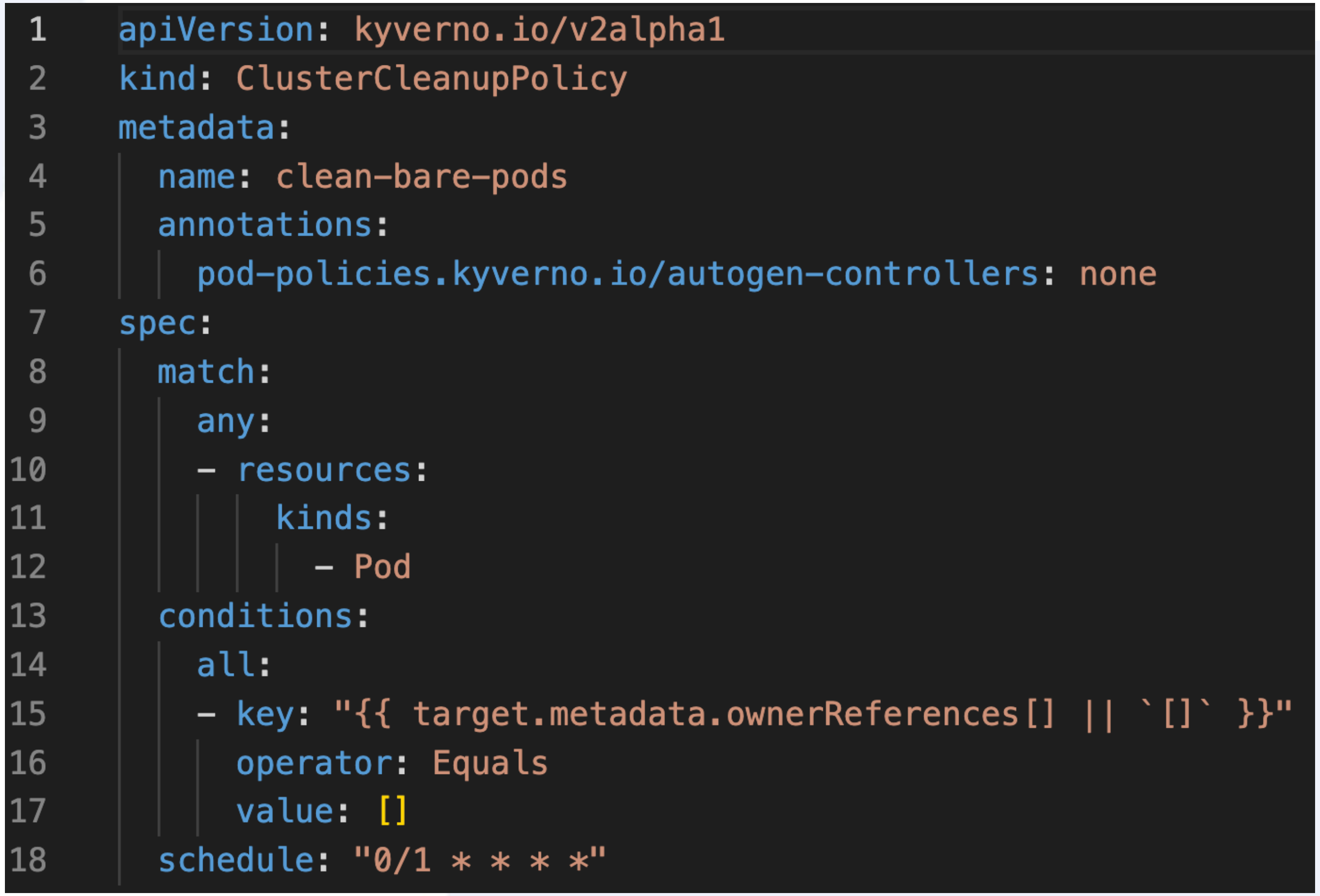
verify_images > check-images.yaml > {} spec > [ ] rules > {} 0 > [ ] verifyImages

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: check-image
spec:
  validationFailureAction: enforce
  background: false
  rules:
    - name: check-image
      match:
        resources:
          kinds:
            - Pod
      verifyImages:
      - image: "ghcr.io/kyverno/test-verify-image:*"
        key: |-
          – ---BEGIN PUBLIC KEY-----
          MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE8nXRh950
          IZbRj8Ra/N9sbqOPZrfM5/KAQN0/KjHcorm/J5yctVd7
          iEcnessRQjU917hmKO6JWVGHpDguIyakZA==
          – ---END PUBLIC KEY--- –

```

Cleanup policies

- Delete resources based on flexible match/exclude and conditions
- Run checks periodically using Cron schedule format



```yaml
apiVersion: kyverno.io/v2alpha1
kind: ClusterCleanupPolicy
metadata:
  name: clean-bare-pods
  annotations:
    pod-policies.kyverno.io/autogen-controllers: none
spec:
  match:
    any:
    - resources:
        kinds:
          - Pod
  conditions:
    all:
    - key: "{{ target.metadata.ownerReferences[] || `[]` }}"
      operator: Equals
      value: []
  schedule: "0/1 * * * *"
```

Demos

Additional Features

Additional Features

- Built-in and Custom Variables
- JMESPath Support
- API Lookups
- Cached ConfigMaps
- OCI Registry integrations
- OpenTelemetry Metrics and Spans
- Policy Reporter (In-cluster dashboard)
- YAML Signing
- Policy Exceptions

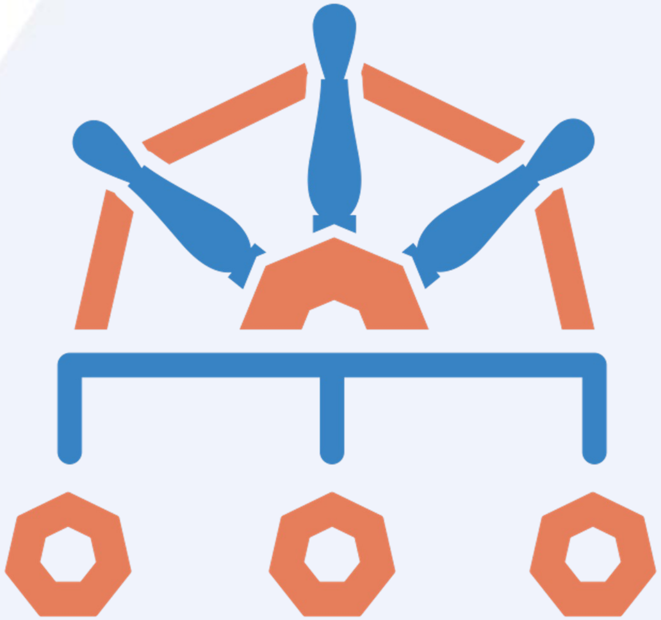
Summary

Key Takeaways

1. Policy is a must have for Kubernetes security and compliance

2. Kyverno is a CNCF policy engine built for Kubernetes

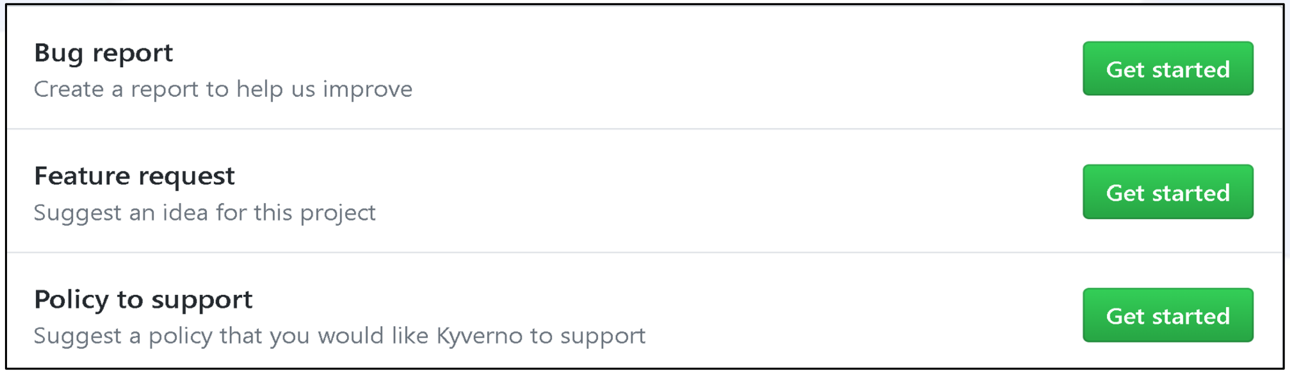
3. Kyverno is easy to get started and try out!



Join the Kyverno Community

- The Kyverno docs & samples: https://kyverno.io
- Slack Channel: https://slack.k8s.io/#kyverno
- Monthly community meetings
- Weekly contributor meetings

Join https://groups.google.com/g/kyverno



Bug report
Create a report to help us improve

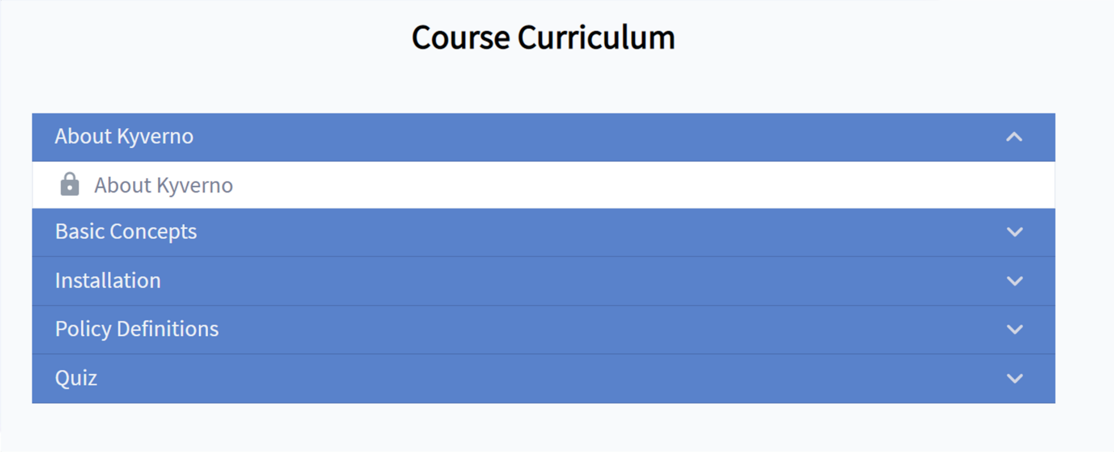
Feature request
Suggest an idea for this project

Policy to support
Suggest a policy that you would like Kyverno to support

Get Kyverno Certified!

- Free training and certification

https://learn.nirmata.com

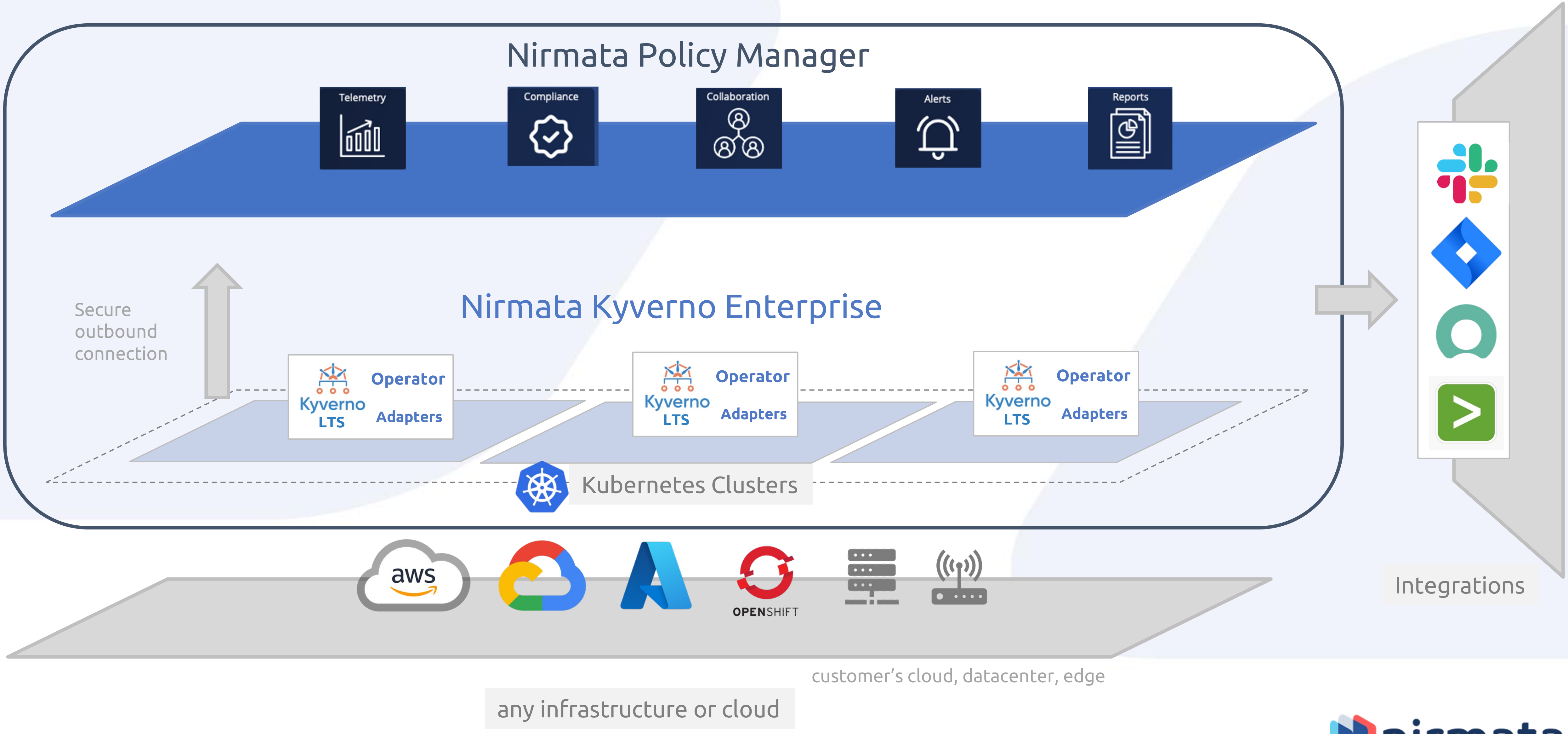


Course Curriculum

- About Kyverno
  - About Kyverno
- Basic Concepts
- Installation
- Policy Definitions
- Quiz

nirmata

Nirmata Architecture



nirmata

Nirmata Enterprise Products

addressing the needs for platform teams

Nirmata for Kyverno OSS

- Use your own fork
- 24x7 emergency support
- Private priority collaboration
- Enablement services for production readiness, assessments, upgrades, trainings

Nirmata Enterprise Kyverno

- Kyverno long term support with compatibility testing and fixes for CVEs and critical bugs
- Quarterly trainings and upgrade support
- Curated policy sets
- Kyverno Operator
- Policy data adapters and Integrations
- 24x7 support

Nirmata Policy Manager

- Includes all Nirmata Enterprise Kyverno features
- Enterprise collaboration & workflows with OIDC/SAML
- Scheduled policy reports with owner assignment
- Policy metrics and health
- Centralized multi-cluster visibility and governance
- Continuous compliance
- Custom integrations available
- Training & services available

Thanks!

https://try.nirmata.io